# Unified Command Management of SAO Computer Systems: The EUCOM Solution

**By**

**Mark Ahles**
**Defense Institute of Security Assistance Management**

A number of articles in the *DISAM Journal* have discussed Security Assistance Office (SAO) and Office of Defense Cooperation (ODC) computer requirements. "Planning, Designing, and Operating Local Area Networks," (*DISAM Journal*, Summer 1997, Vol-19/N-4,p.115-123) dealt with the general requirements for setting up a network of computers in an SAO or ODC. "ODC Information Management," (*DISAM Journal*, Fall 1997, Vol-20/N-2, p. 70-88) looked specifically at one ODCs detailed planning and analysis of their local computer needs. "DISAM Supports Security Assistance Organization's Automation Needs," (*DISAM Journal*, Winter 1999-2000, Vol-22/N4, p.85-88) discussed support DISAM provided in meeting SAO/ODC computer requirements.

These articles have provided good information on SAO/ODC computer needs, but did not directly suggest a detailed road map of exactly what an office needed to do to install, maintain, and pass inspection on their computer systems. Rick Dyer, Training Manager for the U.S. European Command, decided in 1998 to compile all of the guidance in one place for EUCOM SAOs.

With assistance from DISAM, and much hard work from some EUCOM computer experts (Tsgt Don Lewis and Mairi Marquart), EUCOM has just published its *Security Assistance Office Automation Guide* (SAOAG).

The SAOAG provides outstanding guidance from basic conceptual definitions (what is a LAN?) to an actual sample SAO/ODC ADP Plan. Although the EUCOM SAOAG was written specifically for EUCOM, almost all of the guidance contained is valuable to any SAO or ODC.

The guide opens with a general section on information assurance. This section provides good general information on computer use for any office. For example, personal use of government computers states:

> We have detailed rules for appropriate and inappropriate use of government computers. We also have rules governing how you may use your government computer for personal use. The U.S. government provides you with a computer to do your assigned duties. The rules are simple and clear. Government computers may be used only by government employees for the following:
>
> - Official business related to your official duties.
> - Authorized personal use includes brief access and searches for information on the internet and sending short e-mail messages.
> - Security assistance office chiefs and supervisors must make every effort to ensure that personal use of government computers.
>
> •• Does not adversely affect the performance of official duties.

•• Is limited to reasonable duration and frequency and, when possible, done during off-duty hours.

•• Serves a legitimate public interest, such as keeping employees at their desks, furthering the education and self improvement of employees, improving employee morale and welfare, or job-searching in response to downsizing.

•• Personal use of government computers must not overburden the communications system.

•• Personal use of government computers must not reflect adversely on DoD or DoD components.

•• Misuse of government computers includes hacking or using hacker tools, visiting hacker websites, deliberately installing viruses on DoD computers, trying to mask or hide your identity, attempting to bypass security policy, using internet telephony, streaming audio/video (such as receiving hourly stock updates), and using Hotmail, Rocketmail, and Yahoomail for other than morale, welfare, and recreation.

• Penalties for misuse of government computers range from courts-martial to nonjudicial and administrative actions, such as letters of reprimand.

The guide also addresses a number of other often confusing computer use areas. The SAOAG discusses laptop use, problem reporting, computer hoaxes, and other topics. By clearly detailing the restrictions on computer use and the penalties that can result, EUCOM has summarized numerous DoD regulations and messages into a few short, easy to read paragraphs.

The second section of the SAOAG discusses automation hardware. The section does a good job of describing the major pieces of equipment available for most offices. Everything from personal computers to telephones to digital assistance is defined. The buying advice and EUCOM guidance included will also help in making purchasing decisions. The section ends with the following suggest equipment for small to mid size offices.

| | One Person | Three People | Ten People |
|---|---|---|---|
| **Computer** | **1** | **3** | **10** |
| **Printer (BW)** | **1** | **1** | **2** |
| **Printer (Color** | | | **1** |
| **CD-ROM** | | **2** | **8** |
| **CD-Writer** | **1** | **1** | **2** |
| **Scanner** | | **1** | **1** |
| **External Storage Device (Zip/Jazz)** | **1** | **1** | **3** |
| **Laptop** | * | **1** | **2** |
| **Digital Camera** | | **1** | **1** |
| **Modem**** | **1** | **1** | **2** |
| **Fax** | **1** | **1** | **1** |
| **Server** | | *** | **1** |

* May want to consider using docked laptop for a workstation vice a PC.
** The number of modems can be reduced with the use of servers.
*** One of the personal computers can be used as the network server.

Section three continues the explanation of automation requirements by detailing software requirements. This section details what software EUCOM will support. It also details what computer programs EUCOM requires: antivirus software.

Office local area networks are explained in section four. The SAOAG provides details of everything from wire types to server maintenance. Once again, the guide provides an overview of the technology with easy to understand explanations. The purpose is to provide readers with the information needed to make an informed decision on how to implement a local area network for your office. The section closes with specific guidance on what local area networks should work best for most offices (10BaseT Ethernet with a central hub and peer-to-peer networking). The solution proposed is relatively inexpensive to install and support, even in small offices.

The SAOAG continues with a short section describing the methods of internet access an office can consider. The guide describes the pros and cons of both dial-up and direct internet connections.

The remainder of the SAOAG is designed for those who want the "inspection proof" solution. The guide includes a sample SAO/ODC automation plan with:

- Cover and table of contents
- Network diagram
- Hardware inventory
- Software inventory
- Projected requirements
- A Computer-User Agreement.

The documents can be edited for local use and provide the blueprint for any security assistance office or office of defense cooperation automation plan.

The EUCOM SAOAG provides a great starting point for any office's automation plan. The guide summarizes in easily read terms almost everything an office needs to build a plan for local automation.

The SAOAG is available for download in from the security assistance networks http://www.idss.ida.org/san/login EUCOM library.

**About the Author**

Mark Ahles is currently an Associate Professor of Security Assistance at DISAM. His main areas of focus are international training management and related software development. He has previously worked at the National Security Agency, Air Force Logistics Command, and the Air Force Security Assistance Center. Mark Ahles holds a reserve commission of Major. He is currently assigned to the Ohio Army National Guard as the Defense Security Cooperation Agency's National Guard Programs Officer. Mark Ahles has completed Bachelors and Masters Degrees in Computer Science and is presently a Ph.D. student at The Union Institute researching national security computer and information systems.